Progetti di Digital Forensic

Alfredo De Santis

Marzo 2011

Progetti di Digital Forensic

- Windows Forensics (Valerio Cinque, Francesco Testorio, Andrea Di Maio)
- Falso alibi digitale su Windows 7 (Alessandro Bove, Alfonso Martorelli, Giuseppe Valentino, Luigi Di Biasi)
- Distribuzioni Linux per analisi forense (Helix 3, DEFT Linux 6, CAINE, Backtrack)
  - Live forensic (Mario Fiore Vitale, Fabio Fulgido, Gaetano Rocco)
  - Post-mortem forensic (Umberto Annunziata, Claudio Gargiulo)
- Linux Forensics (Domenico Viscito, Fabio Favale)
- Falso alibi digitale su Linux (Antonio Sanfelice, Sara Cantalupo, Demia Massaro, Giovanni Costa)
- iPod ed iPhone Forensics (Giovanni Mastroianni, Luisa Siniscalchi, Domenico Voto)
- Android Forensics (Davide Barbuto, Francesco Capano, Gaetano Contaldi, Andrea Vallati)
- Image Forensics (Giuseppe Lanzilli, Hamza Hamim, Gianluca Roscigno)
- GPS Navigation Devices Forensics (Ermanno Travaglino, Armando Faggiano)
- Investigazione di un Computer (Alessio Marzaioli, Francesco Pisano)
- Network Investigations (Dario Casciello, Domenico Memoli, Antonio Della Sala)
- Social Network Forensics
- Mac OS X Forensics

Organizzazione

- Deliverables:
  - Progetto (word + materiale eventuale di supporto)
  - Presentazione (powerpoint)
  - Pubblicazione versioni pdf sul web
- Chiarezza espositiva
- Approccio top-down
- Struttura progetto:
  - Titolo, nomi (prima pagina)
  - Indice
  - Introduzione
  - Sezioni e sottosezioni
  - Bibliografia
  - Appendici (eventuali)
- Organizzazione interna al gruppo di lavoro
  - Decisa in autonomia, poi resa pubblica

Stati di avanzamento e tempi

- Dopo un mese
  - bozza con indice, struttura, introduzione, referenze
  - Presentazione 10/15 min
- Dopo due mesi
  - intermedia con analisi senza dettagli
  - Presentazione 30 min
- Dopo tre mesi
  - versione finale
  - Presentazione 60/90 min

Indicare esplicitamente ad ogni stato di avanzamento l'organizzazione interna del gruppo

Collaboratori

- Dott. Aniello Castiglione
  - castiglione@ieee.org
- Dott. Bonaventura D'Alessio
  - bdalessio@dia.unisa.it

Fonti

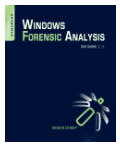
- Fonti autorevoli
- Preferibili libri ed articoli pubblicati su riviste e conferenze scientifiche
- Vediamo qualche esempio

Windows

Eoghan Casey,
Digital Evidence & Computer Crime
Second Edition, 2004, Academic Press
Chapter 10 Forensic examination of Windows Systems

Handbook of Digital Forensics and Investigation
2010, Academic Press
Chapter 5. Windows Forensic Analysis

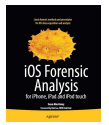
Harlan Carvey
Windows Forensic Analysis DVD Toolkit,
2nd edition, 2009, Syngress



Mac, iPhone, Linux

Mac OS X, iPod, and iPhone Forensic Analysis Toolkit,
Syngress Publishing, 2009

Sean Morrissey,
iOS Forensic Analysis for iPhone, iPad, and iPod touch,
apress, 2010



Handbook of Digital Forensics and Investigation,
Elsevier, 2010

- Chapter 6. UNIX Forensic Analysis
- Chapter 7. Macintosh Forensic Analysis

Network Investigations

Handbook of Digital Forensics and Investigation,
Elsevier, 2010

- Chapter 9. Network Investigations

Android Forensics

Andrew Hoog,
Android Forensics
Syngress, Publication Date: Jun 2011

Jeff Lessard, Gary C. Kessler,
Android Forensics: Simplifying Cell Phone Examinations,
Small Scale Digital Device Forensics Journal, vol. 4, n. 1, Sept. 2010

GPS Navigation Devices Forensics

Chad Strawn,
Expanding the Potential for GPS Evidence Acquisition,
Small Scale Digital Device Forensics Journal, vol. 3, n. 1, June 2009

Tchatchoua Nkwenja Mathia
The Forensic examination of Embedded device such Global Position System (GPS)
Tesi, University of Wales, Newport, UK, 30 April 2009
http://ril.newport.ac.uk/Mathias/finalYrProGPSForensicsExamination.pdf

Clara Maria Colombini,
Sperimentazione di un metodo di analisi forense del dispositivo di navigazione satellitare TomTom,
http://www.iisfa.net/index.php?option=com_docman&task=doc_download&gid=19&Itemid=40

GPSForensic.org
http://www.gpsforensics.org/

Image Forensic

Understanding Forensic Digital Imaging,
Academic Press, Aug 2008

Cynthia Baron,
Adobe Photoshop Forensics Sleuths, Truths, and Fauxtography,
Thompson 2008